

[NEWS] AOL/AIM Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-03/0005.html>

From: support@securiteam.com

Date: 03/02/02

From: support@securiteam.com

To: list@securiteam.com

Date: Sat, 2 Mar 2002 19:55:13 +0100 (CET)

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

When was the last time you checked your server's security?

How about a monthly report?

<http://www.AutomatedScanning.com> – Know that you're safe.

AOL/AIM Vulnerability

SUMMARY

It is possible to retrieve the password of AOL Instant Messenger screen names through the <http://free.aol.com>, <http://www.aol.com>, and <http://www.aim.com> websites. This then leading to possible gain of other accounts such as FTP, e-mail, and so on.

DETAILS

Password retrieval:

AOL Instant Messenger screen names that are registered to the same @aol.com address, but those that no longer exist in AOL's system (Usually 6 months after cancellation/termination of account.) Example: We have an AOL Instant Messenger screen name "hi mom" that is registered under the e-mail hi_mom@aol.com – and since the hi_mom@aol.com account is no longer in AOL's system, it is vulnerable.

Takeover, without current password:

It is possible to take over AOL Instant Messenger screen names that are not currently in AOL's system. Social Engineering is required:

– Visit <http://free.aol.com>

Securiteam: [NEWS] AOL/AIM Vulnerability

– At the first page enter in any information you desire. (Remember this information if you plan on social engineering your way in later.) Now press continues.

– On the next page you will be asked for a screen name and password. Enter in an AOL Instant Messenger screen name and password that you own, that is NOT in AOL's system – Check the check box that says "Check here to use your AIM name on AOL" Now press continue.

– On the next page you will be asked for billing information and a new browser window will pop up. Click the "I Agree" button in the new browser window, it should close. Go back to the initial browser window and press the "Cancel" link on the bottom left hand corner.

– On the next page you will be brought to a new screen that talks about Joining AOL without a credit card. Now press continues.

The next 2 pages will be for verification – keep pressing "Continue" on the next 2 pages until you get to the page that asks for another screen name and password.

If you've done this correctly you will be greeted with "Sorry, <thename> is taken" then asked to enter another screen name and password as stated before. This is where you enter the screen name that you would like to retrieve the password from. (If you enter a screen name that is on AOL already, you will get error saying that it is already taken.) Other errors might occur when trying certain screen names, simply press the back button, and try again.

So, say we enter "S7S Robert" and for the password field you would enter any password (don't forget it, this will be used in the following steps) Press the continue button and if the name was vulnerable you will be taken to a new page and greeted with "Welcome to America Online! Congratulations S7S Robert!" Now we have access to login to the <http://www.aol.com> AOLAnywhere service with the account that was just created.

– Now to retrieve the current password of S7S Robert, we visit <http://www.aim.com> and use the Lost Password feature found under Help. Enter in the screen name of the password to be retrieved and press Submit.

– Visit <http://www.aol.com> to use AOLAnywhere and login to the account using the password you chose before. You should have an e-mail in there from AOL with the password to the screen name.

If you did not receive an e-mail from the Lost Password feature, this means that the AOL Instant Messenger screen name was not registered under the @aol.com address.

From here an attacker could change the password to the AOL Instant Messenger screen name and also try the same password against the victims other accounts.(FTP, SSH, etc)

Securiteam: [NEWS] AOL/AIM Vulnerability

Testing:

To test this simply register an AOL Instant Messenger name at <http://www.aim.com> and when it asks for the e-mail address to use, make it the same as the screen name, and append @aol.com. For instance, if I want to test with "S7S Robert" I would enter the email address S7SRobert@aol.com as well. Once you have done that, you can use the above directions and see that you do not need the password used in the screen name registration process to retrieve it.

Vendor response:

AOL was e-mailed multiple times before this advisory and has yet to receive a reply, so hopefully they are working on it. In the mean time, just make sure your AOL Instant Messenger screen name's email address is not registered to its old @aol.com address.

ADDITIONAL INFORMATION

The information has been provided by <<mailto:robert@sub-seven.com>> Robert Lyttle.

=====

This bulletin is sent to members of the SecuriTeam mailing list.
To unsubscribe from the list, send mail with an empty subject line and body to: list-unsubscribe@securiteam.com
In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====
=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind. In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.

-
- **Previous message:** support@securiteam.com: "[UNIX] IRC Connection Tracking Helper Module (Patch Available)"
 - **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)